UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/903,612	07/13/2001	Yuri Poeluev	67539/00370	2200

27871 7590 03/03/2006

BLAKE, CASSELS & GRAYDON LLP
BOX 25, COMMERCE COURT WEST
199 BAY STREET, SUITE 2800
TORONTO, ON M5L 1A9
CANADA

EXAMINER
ABRISHAMKAR, KAVEH

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/903,612	**Applicant(s)** POELUEV ET AL.	
	Examiner Kaveh Abrishamkar	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 December 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on December 13, 2005 has been entered.

Response to Arguments

2. Applicant's arguments filed December 13, 2005 have been fully considered but they are not persuasive for the following reasons:

Regarding amended independent claim 1, the Applicant argues that the Cited Prior Art (CPA), Badamo et al. (U.S. Patent Publication 2002/0184487), does not teach "encapsulating said at least one encapsulated data packet." This argument is not found persuasive. The specification does not explicitly mention, "encapsulating said at least one encapsulated data packet." Therefore, it is interpreted that the encapsulating of the encapsulated data packet is analogous to adding a PPP header to an IP packet. The CPA discloses that the egress processing system includes encapsulation, PPP generation, and NAT (paragraphs 54 and 55). This encapsulation, PPP generation, and NAT, all involve an encapsulation of the packet as all involve adding headers to the payload. Therefore, there would be at least two headers, and therefore, there is an encapsulation of an encapsulated packet.

Therefore, the rejection is respectfully maintained and applied to the amended claims.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-3, 5, and 8-10 are rejected under 35 U.S.C. 102(e) as being anticipated by Badamo et al. (U. S. Publication 2002/0184487).

4. With respect to claim 1, Badamo et al. disclose a method for providing cryptographic functions to data packets at the PPP layer of a network stack (page 4, column 1, line 19), the method including the steps of:

Intercepting PPP datagrams inbound to said network stack and outbound of network stack (page 4, column 1, lines 15-16), said PPP datagrams having at least one encapsulated data packet encapsulated thereby;

Decapsulating said PPP datagrams to retrieve said at least one encapsulated data packet (page 4, column 1, line 18);

examining said at least one encapsulated data packet to dterine whether to process said at least one encapsulated data packet using said cryptographic functions (page 4, column 1, lines 56-61);

if said at least one encapsulated data packet requires processing, modifying said data packet to provide said cryptographic functions (page 5, column 1, lines 40-42); and

Encapsulating said at least one data packet (page 4, column 1, line 51) for transmission to a next layer of said network stack (page 4, column 1, lines 52-53).

5. With respect to claim 2, Badamo et al. disclose the method of claim, wherein said data packet is an IP packet (page 5, column 1, lines 64-66 to page 5, column 2, lines 1-2. One of average skill in the art is aware that it is inherent in an IP packet to have a header, an address to which the IP packet is sent, and data for which the packet was created.
This inherency is also taught in RFC 791of the IETF, in which they specify a datagram having data and a header in section 2.2, page 9 of the document, and specify the header as having destination and source addresses in section 3, page 14-18 of the document.) having a header, an address and data.

6. With respect to claim 3, Badamo et al. teach the method of claim 1 wherein said step of modifying said data packet includes the further step of selecting an IPSec protocol (page 5, column 1, lines 33-34, 36-37, 41).

7. With respect to claim 5, Badamo et al. disclose a system for processing data packets by providing cryptographic functions to data packets at the PPP layer of a network stack (page 4, column 1, line 19), said system having:

A packet interceptor to intercept PPP datagrams inbound to said network stack and outbound of said stack, said PPP datagrams including at least one IP data packet encapsulated thereby, and to decapsulate said PPP datagrams to retrieve said encapsulated IP data packet (page 4, column 1, lines 43-54);

A security policy manager for storing processing rules for said data packets and selecting at least one of the processing rules for said at least one encapsulated IP data packet (page 6, column 1, lines 20-22); and

A processing module for intercepting and examining said at least one encapsulated IP data packet, and processing said at least one encapsulated IP data packet by selecting and applying said cryptographic functions thereto, said processing module in communication with said security policy manager (items 73 and 74, page 6, column 1, lines 27-29);

Wherein said PPP datagrams are intercepted and examined in accordance with said

processing rules (page 5, column 1, lines 33-34); the IPSec protocol is the protocol from which the processing rules and cryptographic transformations are implemented).

8. With respect to claim 8, Badamo et al. teach the system of claim 5, wherein the cryptographic transformations are implemented using an IPSec protocol by said processing module (page 5, column 1, lines 33-34, 36-37, 41).

18. With respect to claim 9, Badamo et al. teach the system of claim 5, wherein secure communications between correspondents is provided via a virtual private network (page 1, column 2, lines 8-9).

9. With respect to claim 10, Badamo et al. teach a method for providing a cryptographic system for communication between correspondents in a communication network (Fig. 1) to data packets at the PPP layer of a network stack, said method having the step of:

Providing a security module in a computer readable medium (page 4, column 2, lines 3-4 state that the processors that perform the functions of the security module are fast path processor subsystems, and page 5, column 2, lines 3-4 state that fast path coprocessors are microprocessors, which are known in the art to be computer readable mediums.) at each of said correspondents, said security module having:

A packet interceptor to intercept PPP datagrams inbound to said network stack and outbound of said stack, said PPP datagrams including at least one data packet, and to decapsulate said PPP datagrams to retrieve said encapsulated IP packet (page 4, column 1, lines 43-54);

A security policy manager for storing processing rules for said data packets and selecting at least one of the processing rules for said encapsulated data packet (page 6, column 1, lines 20-22)., and

A processing module for intercepting and examining said at least one encapsulated data packet and processing said data packet by selecting and applying said cryptographic transformations on said data packet, said processing module in communication with said security policy manager (items 73 and 74; page 6, column 1, lines 27-29); and

Examining said data packets outbound from said correspondent to determine whether processing by said processing module is required (page 6, column 1, lines 55-58., The ingress and egress processors are used to process incoming and outgoing packets; and

Examining inbound data packets to said correspondent to determine whether processing by said processing module is required by checking whether said data packets include cryptographic functions (page 6, column 1, lines 55-58).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Badamo et al. (U.S. Publication No. 2002/0184487) in view of Ylonen et al. (U.S. Patent 6,438,612).

11. With respect to claim 4, Badamo teaches the limitations of claim 1, from which 4 is a dependent claim. Badamo does not teach the further extrapolation of claim 1, wherein the step of modifying the data packet includes further steps of checking the header information and acting upon said information. Ylonen et al. discloses further steps of modifying the data packet:

Checking header information of outbound packets to the network stack to determine if processing applies (column 8, lines 1 1-15; Ylonen et al. state that the selectors are used to determine if processing applies. According to column 4, lines 61-62, the selectors are specified by the security association. According to column 8, lines 15-18, the values that specify which security association is relevant is obtained in the header of the packet.
Because the selectors are obtained from the security association, and the security association is obtained from the header of the packet, it can be said that the selectors can be obtained from the header of the packet); and

Checking header information of inbound packets to the network stack to determine if the data packets include cryptographic functions (column 8, lines 4-6*, The VNI is selected as a 'selector' in the security association during the negotiation of applying encryption and authentication. The selectors are obtained from the security association, which can be obtained from values designated in the packet header, as mentioned above. By checking if the security association specifies a VNI, the transmitting device is checking the outbound packet's cryptographic functions).

Both Badamo et al. and Ylonen et al. are analogous art because both are in the field of secure communications networks. It would have been obvious to one of average skill in the art at the time of the invention to combine the step of Ylonen et al. with the method of Badamo et al. By doing so, the invention would have error-checking steps, and the likelihood of security problems encountered during or as a result of the invention would be decreased.

12. Claims 6 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Badamo et al. (U.S. Publication No. 2002/0184487) in view of Lantto et al. (U.S. Publication No. 2004/0054794).

13. With respect to claims 6 and 7, Badamo et al. teach the limitations of claim 5, which is the claim upon which claim 6 is dependent. Badamo et al. also teach a packet interceptor located at the PPP layer of the network stack (page 4, column 1, lines 9-11). However, Badamo et al. does not explicitly teach a packet interceptor at the PPP layer as a software module as recited in claim 6, nor does he teach a packet interceptor as a driver in the kernel of an operating system as recited in claim 7. In the Description of Related Ad, Lantto et al. discuss a well-

known prior art network packet interceptor implemented as a software module, more specifically implemented as a driver included in a kernel of an operating system (page 2, column 2, lines 45-49). Both Badamo et al. and Lantto et al. are analogous art because both are in the field of secure communications networks. It would have been obvious to one of average skill in the art at the time of the invention to utilize the kernel-mode driver implementation of a packet interceptor of Lantto et al. with the packet interceptor of Badamo et al. in which the packet interceptor was located at the PPP layer of the network stack because the driver implementation is well-known art that is commercially accepted and used in the field (Lantto et al: page 2, column 2, lines 43-49).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KA
02/22/06

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100